



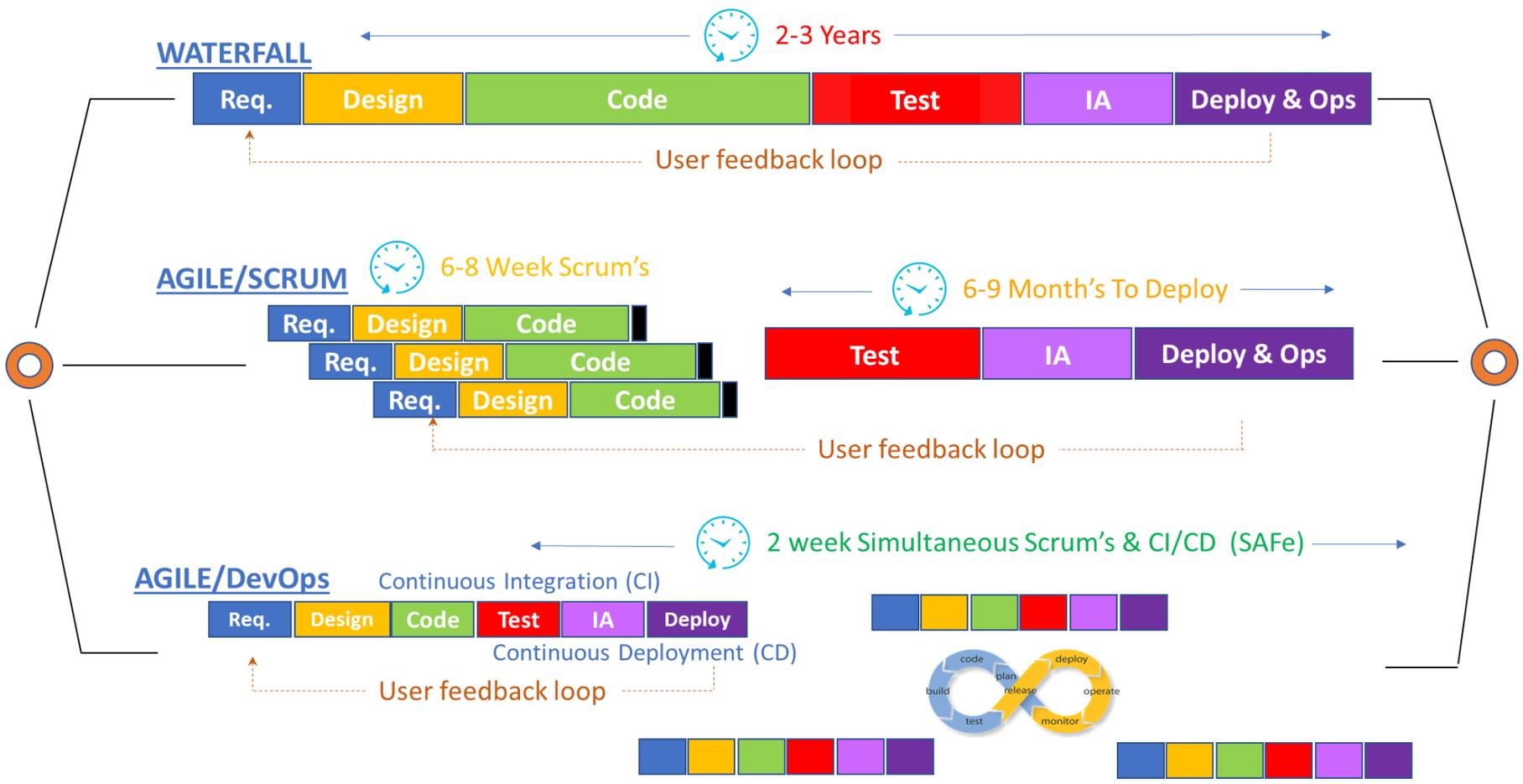
DISA DevSecOps Approach

Agile approach to secure application development

Drew Malloy
SD Tech Director



DISA's Evolution of Application Development





DevSecOps

A **Culture** and a **Mindset** for collaboration between Development and Operations giving you a continuous process that is active throughout the system and application lifecycle.
DevSecOps is Not a Technology!

Keys Tenants

- Development, test, security and operations are all part of the same team
- Automate as much as possible – Don't Repeat Yourself!
- Total visibility throughout the process
- Everything is an artifact of configuration management
- Eliminate waste and reduce bottlenecks
- Emphasize fast feedback
- Deliver a Minimum Viable Product (MVP) with continuous increments thereafter
- Learn from failures and develop a blameless culture
- Expect failure and plan for the contingency
- DevSecOps Process is available in Every Environment – from Development through Production



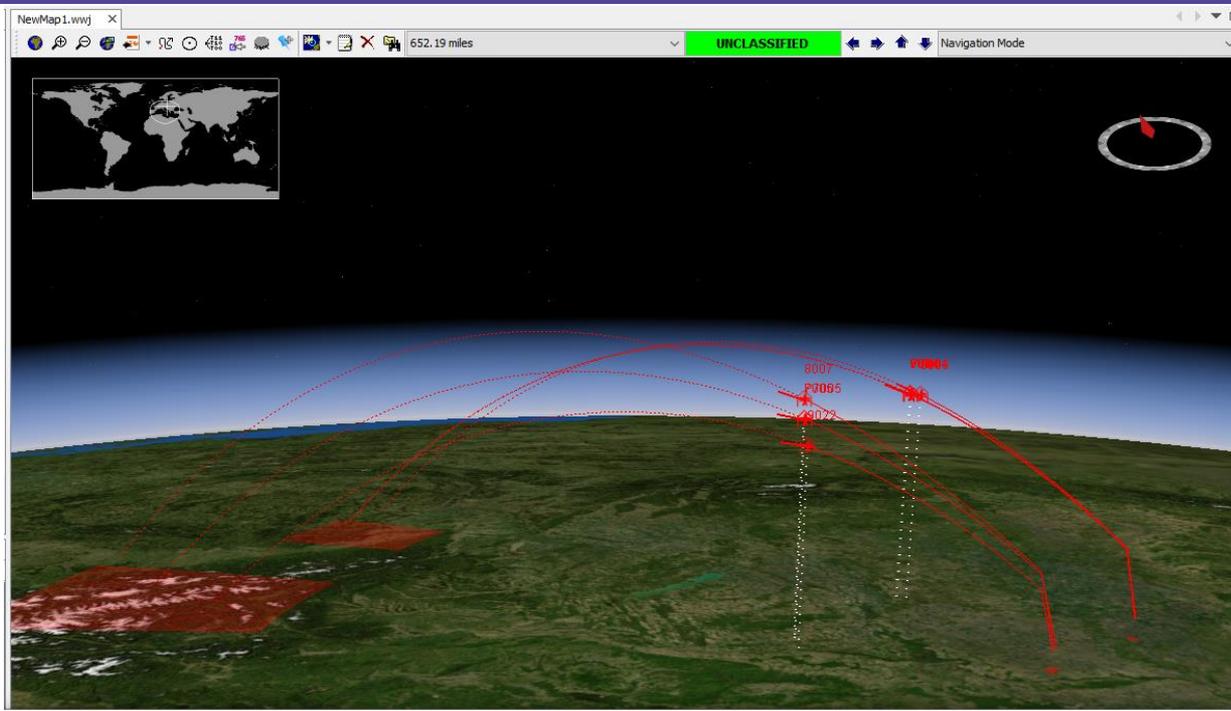
Global Command and Control System – Joint Enterprise (GCCS-JE) Vision

- **Global Command and Control System – Joint Enterprise (GCCS-JE) Vision**
 - GCCS-JE is a modernized information technology solution that provides continuous, timely, secure, and resilient C2 capabilities to the war-fighter in the modern environment. GCCS-JE fuses, distributes, and displays data in a Common Operating Picture, providing situational awareness from strategic to operational levels on a globally accessible cloud based service.





GCCS-JE Acquisition Approach



DevSecOps Process

- Short iterations of capability development (sprints); enables faster delivery of capability to the warfighter

Contracting Vehicles

- Leveraging an OTA vehicle to procure framework development and pipeline.
- **Did not shorten award time!** Did provide access to non-traditional expertise

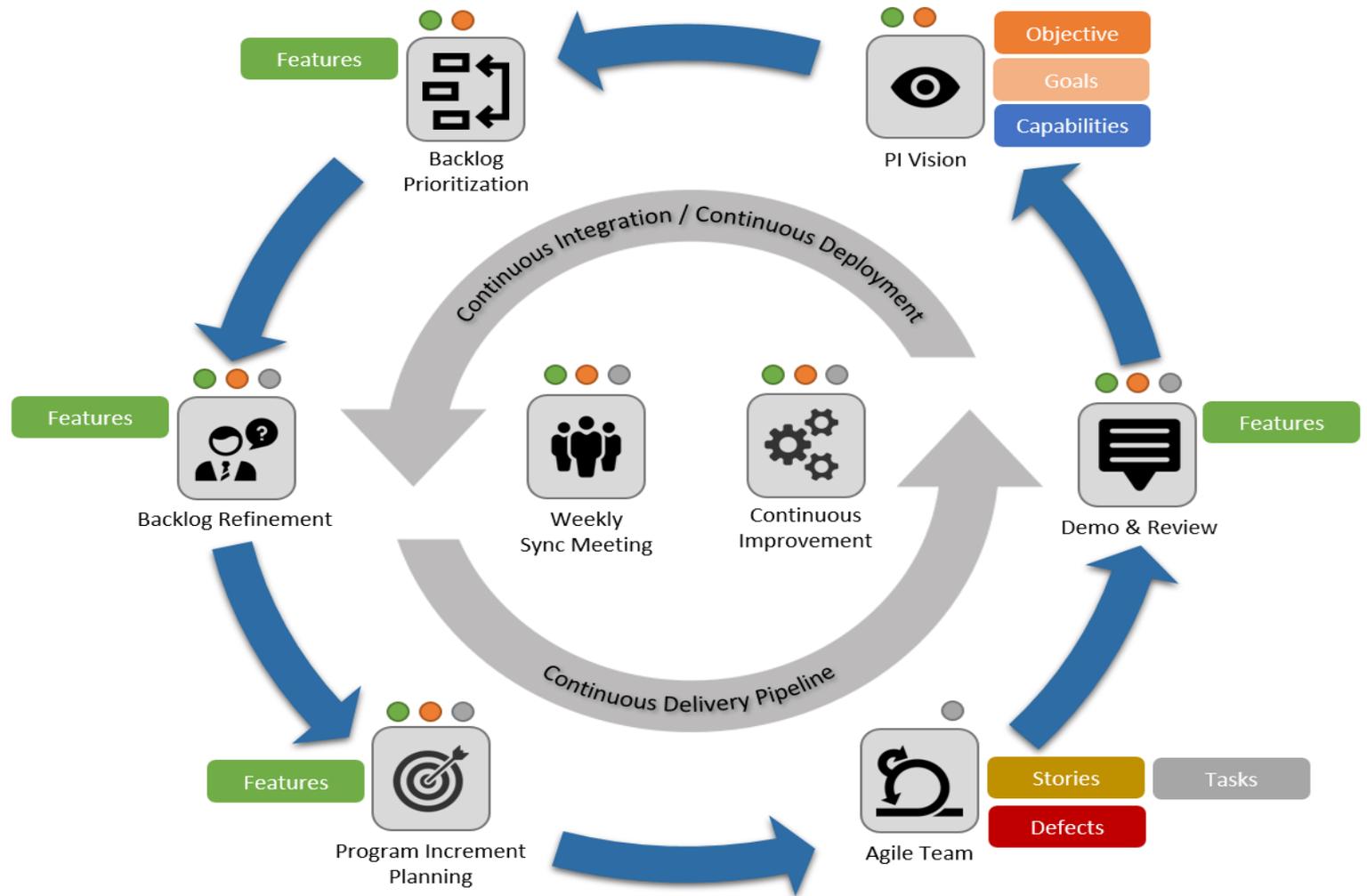
Constant and Frequent Collaboration with Stakeholders

- Provides a better product that is tailored to the feedback of the community



Agile Release Train Framework

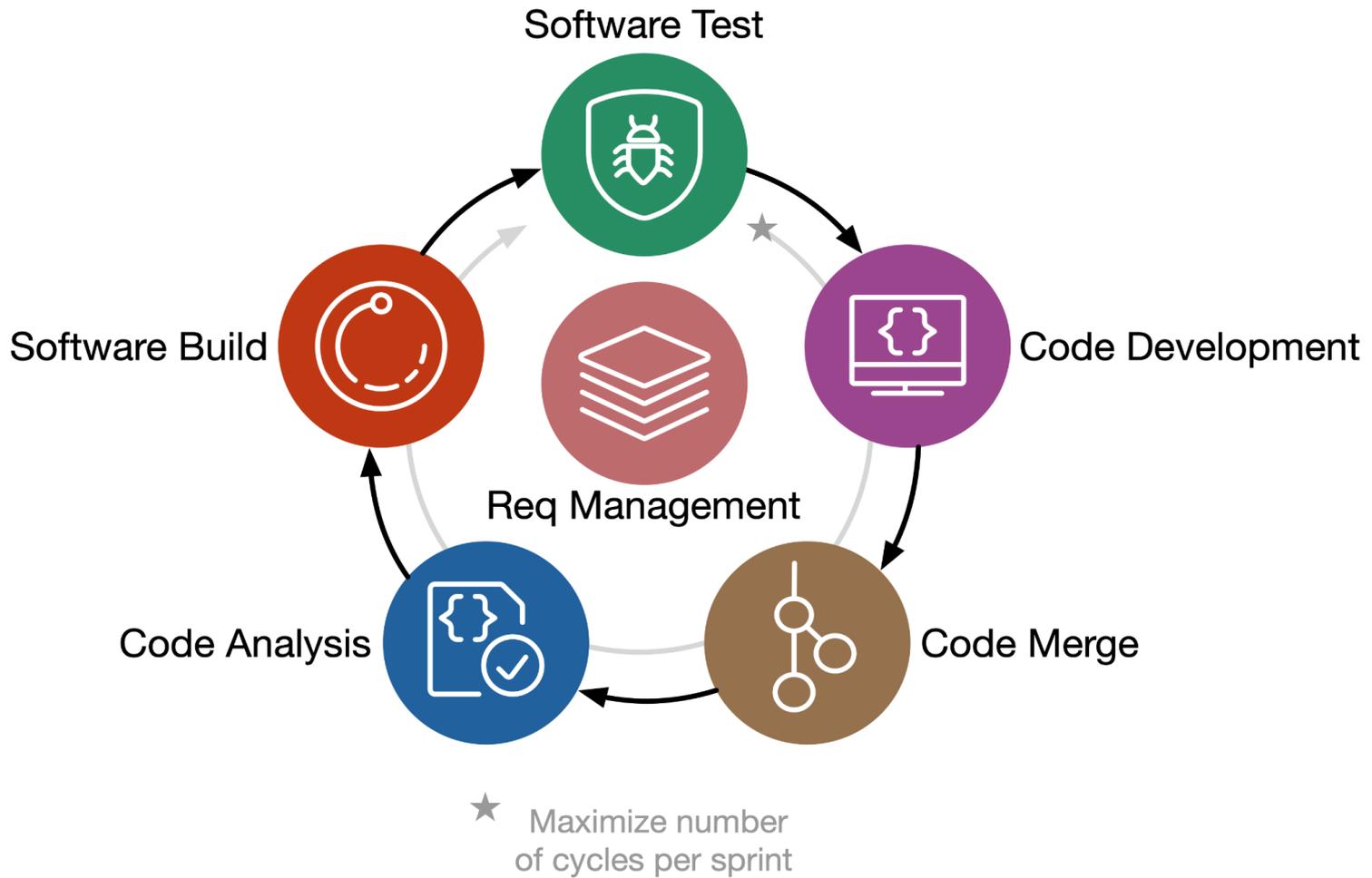
- Governance
- Metrics
- Technical Excellence



- Operational Sponsor
- Program Team
- Development Teams



DevSecOps Process Flow



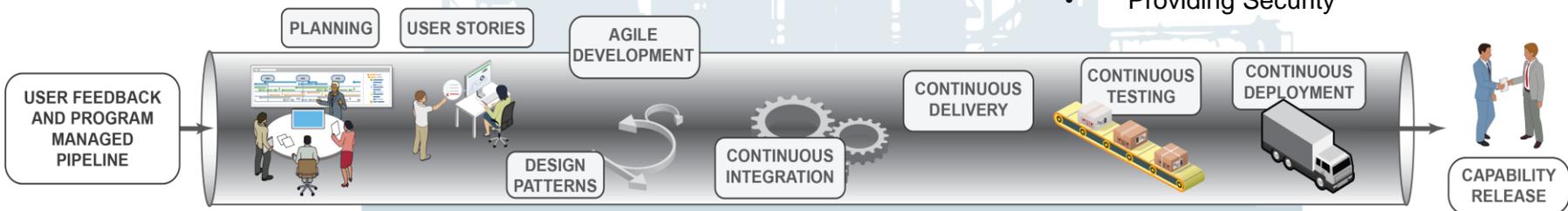


DISA Services Development and Delivery

Development, Test, Security and Operations are all part of the same team

Technical Delivery of Capabilities

- Developing GOTS Solutions
- Integrating Open Source & COTS Products
- Facilitating Collaboration
- Providing Security



ARCHITECTURE, STANDARDS, AND BEST PRACTICES



COTS SOFTWARE CAPABILITIES

VOICE & VIDEO

COLLABORATION SERVICES

PRODUCTIVITY SERVICES

GOTS SYSTEM DEVELOPMENT

SITUATIONAL AWARENESS, FORCE PROTECTION, & INTEL

LOGISTICS

STRATEGIC PLANNING

COTS SOFTWARE & EXTENSIONS

FINANCIAL MANAGEMENT

ACQ&LOG CONTENT & PROGRAM MANAGEMENT

HUMAN RESOURCE MANAGEMENT

ENTERPRISE DATA AND NETWORK FUEL THE POWER OF SERVICES



NIST 800-37 Ongoing Authorization

The vision and intent of NIST Policy as noted in 800-53 supports an **Automated Delivery Pipeline**

Appendix F.4: Ongoing Authorization

“The ultimate objective is to achieve a state of **ongoing authorization** where the authorizing official maintains sufficient knowledge of the current security state of the information system .. to determine whether continued operation is acceptable based on ongoing risk determinations ... Formal reauthorization actions are avoided in situations where the continuous monitoring process provides authorizing officials the necessary information to manage the potential risk...”

Appendix G: Continuous Monitoring

“The monitoring program is integrated into the organization’s system development life cycle processes...Near real-time risk management of information systems can be facilitated by employing automated support tools to execute various steps in the RMF **including authorization-related activities.**”

Ref: NIST 800-37: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf>



Secure Agile

+

DevOps

+

Continuous
Monitoring

=

Ongoing
Authorization



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

 www.disa.mil  /USDISA  @USDISA



visit us

DISA Booth **1929**

follow us



Facebook/USDISA



Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at www.disa.mil/about/industry-partners.